PCT/ E S 03 / 0 0 0 08 #0
10/501211

MINISTERIO
DE CIENCIA
Y TECNOLOGIA

Oficina Española
de Patentes y Marcas

REC'D 09 APR 2003
WIPO PCT

CERTIFICADO OFICIAL

Por la presente certifico que los documentos adjuntos son copia exacta de la solicitud de PATENTE de INVENCION número 200200070, que tiene fecha de presentación en este Organismo el 15 de Enero de 2002.

Madrid, 20 de marzo de 2003

El Director del Departamento de Patentes
e Información Tecnológica.

P.D.

M. MADRUGA

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

MINISTERIO DE CIENCIA Y TECNOLOGIA

Oficina Española de Patentes y Marcas

INSTANCIA DE SOLICITUD

NUMERO DE SOLICITUD: P200200070

02 ENE 15 12:07

FECHA Y HORA DE PRESENTACIÓN EN LA O.E.P.M.

FECHA Y HORA PRESENTACIÓN EN LUGAR DISTINTO O.E.P.M.

(1) MODALIDAD
[X] PATENTE DE INVENCIÓN [ ] MODELO DE UTILIDAD

(2) TIPO DE SOLICITUD
[ ] ADICIÓN A LA PATENTE
[ ] SOLICITUD DIVISIONAL
[ ] CAMBIO DE MODALIDAD
[ ] TRANSFORMACIÓN SOLICITUD PATENTE EUROPEA
[ ] PCT: ENTRADA FASE NACIONAL

(3) EXPED. PRINCIPAL O DE ORIGEN:
MODALIDAD
NUMERO SOLICITUD
FECHA SOLICITUD

(4) LUGAR DE PRESENTACIÓN: Madrid — CÓDIGO: 28

(5) SOLICITANTE(S): APELLIDOS O DENOMINACIÓN SOCIAL	NOMBRE	NACIONALIDAD	CÓDIGO PAIS	DNI/CIF	CNAE	PYME
UNIVERSITAT POLITÈCNICA DE CATALUNYA				Q-0818003-F		

(6) DATOS DEL PRIMER SOLICITANTE

DOMICILIO	Jordi Girona Salgado, 31. Edif. C-H	TELEFONO	902194278
LOCALIDAD	BARCELONA	FAX	93/2400051
PROVINCIA	BARCELONA	CORREO ELECTRONICO	mrsl@dracnet
PAIS RESIDENCIA	ESPAÑA	CÓDIGO POSTAL	08034
NACIONALIDAD	ESPAÑA	CÓDIGO PAIS	ES
		CÓDIGO NACION	ES

(7) INVENTOR (ES): APELLIDOS	NOMBRE	NACIONALIDAD	CÓDIGO PAÍS
RICO NOVELLA	FRANCISCO JOSE	ESPAÑOLA	ES

(8)
[ ] EL SOLICITANTE ES EL INVENTOR
[X] EL SOLICITANTE NO ES EL INVENTOR O ÚNICO INVENTOR

(9) MODO DE OBTENCIÓN DEL DERECHO:
[X] INVENC. LABORAL [ ] CONTRATO [ ] SUCESIÓN

(9) TÍTULO DE LA INVENCIÓN
PROCEDIMIENTO DE EXPEDICION Y VALIDACION DE DOCUMENTOS

(11) EFECTUADO DEPÓSITO DE MATERIA BIOLÓGICA: [ ] SI [X] NO

(12) EXPOSICIONES OFICIALES: LUGAR — FECHA

(13) DECLARACIONES DE PRIORIDAD: PAIS DE ORIGEN	CÓDIGO PAÍS	NÚMERO	FECHA

(14) EL SOLICITANTE SE ACOGE AL APLAZAMIENTO DE PAGO DE TASAS PREVISTO EN EL ART. 162. LEY 11/86 DE PATENTES [X]

(15) AGENTE/REPRESENTANTE: NOMBRE Y DIRECCIÓN POSTAL COMPLETA. (SI AGENTE P.I., NOMBRE Y CÓDIGO) (RELLÉNSE, ÚNICAMENTE POR PROFESIONALES)
MORGADES MANONELLES, JUAN ANTONIO, 323/9, Rector Ubach, 37-39 bj.2ª, BARCELONA, BARCELONA, 08021

(16) RELACIÓN DE DOCUMENTOS QUE SE ACOMPAÑAN:
[X] DESCRIPCIÓN. Nº DE PÁGINAS: 19
[X] Nº DE REIVINDICACIONES: 8
[ ] DIBUJOS. Nº DE PÁGINAS:
[ ] LISTA DE SECUENCIAS Nº DE PÁGINAS:
[X] RESUMEN
[ ] DOCUMENTO DE PRIORIDAD
[ ] TRADUCCION DEL DOCUMENTO DE PRIORIDAD
[ ] DOCUMENTO DE REPRESENTACIÓN
[ ] JUSTIFICANTE DEL PAGO DE TASAS DE SOLICITUD
[ ] HOJA DE INFORMACIÓN COMPLEMENTARIA
[ ] PRUEBAS DE LOS DIBUJOS
[ ] CUESTIONARIO DE PROSPECCIÓN
[ ] OTROS:

FIRMA DEL SOLICITANTE O REPRESENTANTE
JUAN ANTONIO MORGADES MANONELLES
(VER COMUNICACIÓN)

FIRMA DEL FUNCIONARIO

NOTIFICACIÓN DE PAGO DE LA TASA DE CONCESIÓN:
Se le notifica que esta solicitud se considerará retirada si no procede al pago de la tasa de concesión; para el pago de esta tasa dispone de tres meses a contar desde la publicación del anuncio de la concesión en el BOPI, más los diez días que establece el art. 81 del R.D. 2245/1986

ILMO. SR. DIRECTOR DE LA OFICINA ESPAÑOLA DE PATENTES Y MARCAS

Informacion@oepm.es
www.oepm.es
C/ PANAMÁ, 1 • 28071 MADRID

MOD. 3101 - 1- EJEMPLAR PARA EL EXPEDIENTE

NO CUMPLIMENTAR LOS RECUADROS ENMARCADOS EN ROJO

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

NUMERO DE SOLICITUD

P200200970

FECHA DE PRESENTACION

HOJA INFORMACIONES COMPLEMENTARIAS

☐ PATENTE DE INVENCION
☐ MODELO DE UTILIDAD.

(4) SOLICITANTES	APELLIDOS O RAZON SOCIAL	NOMBRE	DNI

(6) INVENTORES	APELLIDOS	NOMBRE	NAC.
- FORGA ALBERICH		JORDI	ES
- SANVICENTE GARGALLO		EMILIO	ES
- MATA DIAZ		JORGE	ES
- DE LA CRUZ LLOPIS		LUIS JAVIER	ES
- ALINS DELGADO		JUAN JOSE	ES

(11) EXPOSICIONES OFICIALES

LUGAR:	FECHA:

(12) DECLARACIONES DE PRIORIDAD

PAIS DE ORIGEN	CODIGO	NUMERO	FECHA

MINISTERIO DE CIENCIA Y TECNOLOGÍA

Oficina Española de Patentes y Marcas

NÚMERO DE SOLICITUD

P200200070

FECHA DE PRESENTACIÓN

15 ENE. 2002

RESUMEN Y GRÁFICO

RESUMEN (Máx. 150 palabras)

"PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS"

Se realiza mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas. Se caracteriza en que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

GRÁFICO

(VER INFORMACIÓN)

MINISTERIO
DE CIENCIA
Y TECNOLOGÍA

Oficina Española
de Patentes y Marcas

(12) **SOLICITUD DE PATENTE DE INVENCIÓN**

(21) NÚMERO DE SOLICITUD P 20 0200070

(22) FECHA DE PRESENTACIÓN 15 ENE. 2002

(62) PATENTE DE LA QUE ES DIVISIONARIA

DATOS DE PRIORIDAD

(31) NÚMERO | (32) FECHA | (33) PAÍS

(71) SOLICITANTE (S)
UNIVERSITAT POLITÈCNICA DE CATALUNYA

DOMICILIO Jordi Girona Salgado, 31. Edif. C-H
BARCELONA

NACIONALIDAD ESPAÑA
08034 BARCELONA ESPAÑA

(72) INVENTOR (ES) FRANCISCO JOSE RICO NOVELLA , JORDI FORGA ALBERICH, EMILIO SANVICENTE GARGALLO, JORGE MATA DIAZ, LUIS JAVIER DE LA CRUZ LLOPIS, JUAN JOSE ALINS DELGADO

(51) Int. Cl.[7]
G06F 17/60, H04L 9/00

GRÁFICO (SÓLO PARA INTERPRETAR RESUMEN)

(54) TÍTULO DE LA INVENCIÓN
PROCEDIMIENTO DE EXPEDICION Y VALIDACION DE DOCUMENTOS

(57) RESUMEN

"PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS"

Se realiza mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas. Se caracteriza en que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

PRIMERA PÁGINA DE LA MEMORIA

La presente solicitud de Patente de Invención consiste, conforme indica su enunciado, en un "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS", con el cual resulta imposible la duplicación operativa de los mismos de manera fraudulenta. Tal como se detallará en lo sucesivo, el procedimiento que se describirá a continuación ofrece numerosas ventajas.

Aunque en la presente memoria se hace referencia esencialmente al caso en el que los documentos que se desean obtener son tickets, se entiende que el procedimiento objeto de la presente invención también es aplicable a otros tipos de documentos más generales, tal como se explicará más adelante.

Hoy en día es posible el encargo o la reserva de tickets tales como billetes de avión, billetes de tren, localidades de espectáculos y similares mediante sistemas de tele-venta. El procedimiento para el pago de los mismos es variado, pudiéndose realizar mediante el cargo a una tarjeta de crédito, a una cuenta a través de una entidad bancaria o similar.

Sin embargo, para recoger el ticket comprado de este modo era necesario que éste fuera enviado al destinatario por correo o mediante un servicio de mensajería, lo cual suponía un aumento en los costes de emisión y una incomodidad para el usuario si debía desplazarse para recoger los tickets.

Hasta ahora, la recogida del ticket se venía realizando de esta manera debido principalmente al hecho de que la autenticidad de este tipo de documento está basada en alguna característica del soporte (el papel) o del método de impresión para dificultar la falsificación del mismo. Esto impide que sea el propio usuario el que pueda obtener una copia impresa del documento.

Como alternativa a este procedimiento la técnica anterior propone diversos sistemas de expedición de

tickets de manera remota, los cuales se describen resumidamente a continuación.

Un primer sistema es el que se describe, en mayor o menor medida, en los documentos nº WO01/61577 A2, WO00/74300 A1, WO00/45348, WO200161577,WO2000744300, WO200045348, US5598477, el cual está basado esencialmente en la codificación de los datos que se consideran relevantes y su posterior cifrado, bien mediante técnicas de clave simétrica o asimétrica. El resultado de dicho cifrado se imprime en forma de código de barras o similar para poder realizar una comprobación automática cuando el ticket haya de ser validado. Este sistema imposibilita la generación de tickets por quien desconoce la clave de cifrado (si se usa criptografía de clave asimétrica, la clave secreta del algoritmo). Sin embargo, presenta el inconveniente de que es posible realizar copias de un ticket ya emitido y, por lo tanto, resulta necesario utilizar mecanismos adicionales de seguridad, tal cómo el control en línea de los tickets validados, la inclusión de información personal contrastable (DNI, pasaporte o similar) en el código cifrado (para aquellos tickets que presenten una fecha y un lugar fijos de utilización), etc. Este sistema es especialmente ineficaz en el caso de tickets que pueden ser utilizados en múltiples lugares y en un amplio abanico de fechas, como pueden ser bonos de noche en hoteles, bonos de transporte público, etc, así como en lugares de afluencia masiva, en los que el tiempo requerido para la comprobación de la identidad del portador resulta un serio inconveniente. Por todos estos motivos, este sistema no ha tenido demasiada implantación en la práctica.

Otro sistema es el que se describe, en mayor o menor medida, en los documentos nº EP0969426 A1, EP0829828 A, EP969426, JP11306397, EP309318 y otros, el cual está basado en la grabación, en un dispositivo del tipo tarjeta

inteligente, de la información del ticket. Debido a que el dispositivo de grabación (tarjeta) permite el uso de técnicas criptográficas para la identificación fuerte y presenta una gran robustez frente a la violación de la información que almacena, resulta prácticamente imposible duplicar el ticket, quedando la unicidad del mismo garantizada. Por lo tanto, resultan innecesarios tanto el control en línea de la validación del ticket como la identificación del portador cuando se consume. Sin embargo, este sistema presenta el inconveniente de que requiere que el usuario disponga de un periférico de grabación de tarjetas inteligentes en su casa, lo que encarece en gran medida el coste del sistema y hace que en la práctica no se utilice.

Una alternativa a los sistemas de expedición de tickets de manera remota es la que se propone con el nuevo procedimiento objeto de la presente invención, con el cual se consigue solventar los inconvenientes de los sistemas conocidos. La invención propone un nuevo procedimiento para la obtención de documentos (por ejemplo, tickets) típicamente en casa del usuario y su posterior validación automática. Con el procedimiento de la invención ya no es posible la duplicación operativa de los mismos (garantiza la unicidad) y hace innecesario que el usuario disponga de un lector/grabador de tarjetas inteligentes, lo que abarata y flexibiliza el sistema.

El procedimiento de la invención utiliza técnicas criptográficas robustas en conjunción con dispositivos verificadores portátiles, los cuales poseen capacidad de procesado y almacenamiento de información, presentan un alto grado de protección frente a lecturas y escrituras desautorizadas y dificultan en gran medida la duplicación fraudulenta.

Unos dispositivos verificadores portátiles que resultan especialmente adecuados son las tarjetas

inteligentes.

Aunque teóricamente resulta más adecuado el uso de criptografía de clave pública para la obtención de códigos de autenticidad (pues ello permite que en la fase de validación no se tengan que almacenar claves secretas), el tamaño de los códigos resultantes es sensiblemente superior al necesario si se emplea criptografía de clave secreta (simétrica). Si la forma final del documento no es impresa (soporte magnético, óptico, electrónico, etc.) este hecho no presenta mayor relevancia, pero si el documento ha de imprimirse, la lectura automática del código de autenticidad obligaría al uso de códigos de puntos, cuya lectura requiere aparatos más caros. Por este motivo, y para facilitar el soporte impreso, se prefiere el uso de criptografía de clave simétrica. Como contrapartida se tienen que utilizar dispositivos de almacenamiento seguro de claves en los verificadores, típicamente microprocesadores de seguridad.

La invención constituye un sistema seguro de expedición remota(típicamente por Internet desde un navegador) de documentos (típicamente tickets) y su validación mediante lectores automáticos (típicamente lectores de códigos de barras) capaces de leer/escribir en los dispositivos verificadores portátiles (típicamente tarjetas inteligentes). Por motivos de rapidez de lectura, robustez y versatilidad es recomendable que los dispositivos verificadores portátiles permitan la operación sin contactos.

Los elementos que intervienen en todo el procedimiento de la invención son los siguientes:

- emisor de dispositivos verificadores portátiles: es el encargado de proporcionar los dispositivos verificadores portátiles necesarios para la validación de los documentos.
- operador de dispositivos verificadores

portátiles: realiza la parte del cifrado del documento que será descifrado por el dispositivo verificador portátil. Para poder realizar esta función las claves correspondientes deben de ser cargadas en el dispositivo verificador portátil. Un dispositivo verificador portátil puede soportar varios operadores de dispositivos verificadores portátiles. Un operador de dispositivo verificador portátil puede coincidir con un emisor.

- portal de documentos: es el encargado de proporcionar el interfaz necesario para la selección y, si procede, la compra del documento. Una vez seleccionado el documento el portal envía a un operador de lector la información adecuada para que sea cifrada con la clave del grupo de lectores/verificadores/grabadores que serán los encargados de validar el documento.

- operador de lector: es el encargado de realizar la parte del cifrado del documento que será descifrada por el citado grupo de lectores/verificadores/grabadores que serán los encargados de validar el documento. El operador de lector es el encargado de la gestión de las claves almacenadas en los lectores/verificadores/grabadores. Un operador de lector puede coincidir con un portal.

- lector/verificador/grabador: es el encargado de leer el código de autenticidad del documento, transmitirlo al dispositivo verificador portátil, recibir su respuesta, descifrarla con la clave correspondiente al operador de lector y validar o rechazar el documento.

- dispositivo verificador portátil: es el encargado de recibir el código de autenticidad del documento (transmitido por el lector/verificador/grabador), y si no ha sido previamente cancelado, descifrar con la clave correspondiente al operador de dispositivos verificadores portátiles, incluirlo en su lista de cancelaciones y enviar al

lector/verificador/grabador el resultado del descifrado.

El procedimiento de expedición y validación de documentos objeto de la presente invención se lleva a cabo mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas.

La particularidad de este procedimiento reside en el hecho de que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

El procedimiento de expedición y validación de documentos comprende las etapas de:

- generación del documento desde un portal de documentos codificándose los datos que se consideren relevantes para realizar una primera operación criptográfica con la clave correspondiente de un grupo de lectores/verificadores/grabadores que participan en la validación del documento y, concatenada a la primera, una segunda operación criptográfica que incluye la clave correspondiente del dispositivo verificador portátil asociado al documento, constituyendo el resultado de dichas operaciones criptográficas un código de autenticidad del documento incorporado al mismo; y

- comprobación del documento que comprende la lectura del código de autenticidad del mismo, realizándose unas terceras operaciones criptográficas adecuadas para la

verificación de las utilizadas en la generación del documento, siendo imprescindible la participación activa del dispositivo verificador portátil asociado para la validación del documento y almacenando el verificador portátil una lista de los documentos que ha verificado de manera que es posible saber, al menos, si se trata de la primera validación.

De acuerdo con una realización de la invención, la individualización de los dispositivos verificadores portátiles se realiza almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las de un algoritmo de cifrado simétrico o de clave secreta. Además, dicha primera y segunda operación criptográfica comprenden dos cifrados mediante un algoritmo criptográfico simétrico, uno con la clave del grupo de lectores/verificadores/grabadores que participan en la validación del documento y otro con la clave correspondiente del dispositivo verificador portátil asociado al documento; y las terceras operaciones criptográficas comprenden el descifrado, por parte del dispositivo verificador portátil con su clave correspondiente, del código de autenticidad del documento y el descifrado subsiguiente, por parte del citado lector/verificador/grabador con su clave correspondiente, realizándose ambos descifrados mediante algoritmos criptográficos simétricos.

Preferiblemente, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública. La citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende una firma digital con una clave secreta, de la cual los citados lectores/verificadores/grabadores que participan en la

validación del documento conocen su correspondiente pública, y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y las terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una comprobación de firma, con la clave pública correspondiente almacenada en los lectores/verificadores/grabadores.

Alternativamente, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública. Dicha citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende un cifrado con la clave pública de los lectores/verificadores/grabadores que participan en la validación del documento y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento. Las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una descifrado con la clave secreta de dichos lectores/verificadores/grabadores.

De acuerdo con otra característica alternativa de la presente invención, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública. La primera y segunda operación criptográfica se basan en criptografía de clave pública que comprende una firma digital con la

clave secreta correspondiente a la clave pública almacenada en los citados lectores/verificadores/grabadores que participan en la validación del documento y otra firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento, y las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende la comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y otra comprobación de firma con la clave pública correspondiente de los lectores/verificadores/grabadores.

Otra alternativa es que la individualización de los dispositivos verificadores portátiles se lleve a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública y que la primera y segunda operación criptográfica se basen en criptografía de clave pública que comprende un cifrado con la clave pública correspondiente a la clave secreta almacenada en dichos lectores/verificadores/grabadores que participan en la validación del documento y una firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y que dichas terceras operaciones criptográficas se basen en criptografía de clave pública que comprende una comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y un descifrado con la clave secreta correspondiente de los citados lectores/verificadores/grabadores.

Adicionalmente, el procedimiento de la invención también comprende la comprobación, antes de validar el

información admitiendo o rechazando el documento e informando de la causa.

Ventajosamente, las claves del lector/verificador/grabador son comunes a un conjunto de lectores.

Las claves almacenadas en los lectores/verificadores/grabadores se obtienen cifrando sus identificadores o parte de ellos con unas claves maestras elegidas por sus operadores.

Si los documentos presentan fecha de caducidad, ésta se incorpora en el código de autenticidad, de manera que pueden ser eliminados de la lista de documentos validados almacenada en dicho verificador portátil una vez que éstos han caducado.

Por otra parte, los citados dispositivos verificadores portátiles adquieren la fecha para borrar los documentos caducados de la lista de documentos validados por medio de un certificado digital emitido por una entidad competente.

La selección y obtención del documento y/o su código de autenticidad puede realizarse a través de Internet y el código de autenticidad del documento se puede enviar al teléfono móvil del usuario o una agenda electrónica o similar del usuario.

De acuerdo con otra característica de la invención, el código de autenticidad puede imprimirse mediante uno o varios códigos de barras. En el caso de varios códigos, éstos incluyen el orden correcto de lectura. Se prevé también que el código de autenticidad pueda imprimirse mediante un código alfanumérico o un código de puntos. El código de autenticidad puede imprimirse también en modo alfanumérico para poder realizar una entrada manual del mismo en caso de deterioro del código de lectura automática.

El procedimiento descrito garantiza la

sistema de clave pública. Dicho certificado, que puede ser emitido una única vez al día, se pasa al dispositivo verificador portátil que, después de comprobar su autenticidad, elimina de la lista los documentos cancelados que ya hayan caducado según la fecha certificada. Naturalmente un documento caducado no será nunca aceptado como válido.

Se trata de un sistema universal para múltiples servicios (espectáculos, transportes, abonos, cupones, cheques, boletos de lotería...), múltiples portales de Internet y múltiples operadores de dispositivos verificadores portátiles. Aunque el sistema es particularmente útil para el formato impreso de los documentos, puede ser utilizado en otros tipos de formatos, como por ejemplo disquetes, almacenamiento en teléfonos móviles, agendas electrónicas portátiles o similares, tarjetas Bluetooth, discos ópticos, CDs, etc.

La alternativa del teléfono móvil o de la agenda electrónica es especialmente interesante, ya que nada impide enviar el código de autenticidad del documento al teléfono móvil del comprador mediante, por ejemplo un SMS o tecnología WAP, y que a la hora de hacer valer dicho documento el comprador lo descargue en el lector/verificador/grabador a través de un enlace infrarrojo, radio (por ejemplo Bluetooth, SMS, etc.) o similar.

En este caso, como ya se ha indicado, la limitación la longitud del código de barras ya no es tal, por lo que podría utilizarse criptografía de clave pública sin problemas.

Se describe a continuación la manera de utilizar la criptografía pública para generar el código de autenticidad.

En primer lugar se selecciona la información relevante, se codifica y se firma digitalmente con la

claves adecuadas. La transmisión se realiza por Internet mediante SSL para garantizar la integridad y la autenticidad de la misma.

El operador de tarjeta y lector realiza un primer cifrado DES Triple de los datos recibidos con la clave del grupo de lectores indicados. Puesto que el tamaño de bloque del algoritmo es de 64 bits, se realiza el cifrado encadenado en modo CBC de los dos bloques (128 bits). La clave del lector la obtiene cifrando (DES Triple) el identificador del lector con una clave maestra que sólo él conoce. Luego realiza un segundo cifrado DES Triple (también encadenado CBC) con la clave de la tarjeta inteligente del portador del ticket, que puede obtenerla, de manera análoga a la del lector, cifrando el identificador de tarjeta con una clave maestra. El resultado de estos dos cifrados es un bloque de 128 bits que constituye el código de autenticidad del ticket. Dicho código se devuelve al portal también vía SSL.

El portal de ticket genera una versión PDF del ticket que contiene, en dos códigos de barras de tipo code128, el código de autenticidad. El motivo por el que se usan dos códigos es que, para una resolución de impresión de 300 ppp, la longitud de un código de barras code128 es de unos 75 mm para una información aproximada de 64 bits, que se corresponde con la máxima anchura admitida por los lectores de códigos de barras económicos. Los códigos incluyen una información en claro de manera que hace irrelevante el orden de lectura de los mismos. El ticket también incluye una trascripción numérica de la información de los códigos, de manera que si éstos se deterioran, dicha información pueda ser introducida manualmente.

El ticket en formato PDF se envía al comprador del mismo, el cual puede imprimirlo en el acto en una impresora estándar.

Una vez en la entrada del espectáculo, el portador del ticket lo entrega junto con su tarjeta al portero. El portero lee el código de barras y a continuación acerca la tarjeta inteligente al lector/grabador sin contactos. La información del código de barras se transfiere en ese momento a la tarjeta, que comprueba que no esté en su lista de tickets ya cancelados. Si lo estuviese, indicaría al lector tal hecho, para que el portero pueda actuar adecuadamente. Si el ticket no se encuentra en la lista de cancelados, lo añade a dicha lista, lo descifra con su clave y lo envía al lector. El lector lo descifra a su vez con su clave secreta y comprueba que los datos sean consistentes (fecha, sesión, asiento, etc.) Si así sucede, valida definitivamente la entrada al espectáculo. Antes de realizarse la transferencia de datos entre lector y tarjeta, se establece una identificación mutua fuerte basada en retos y se establece una clave de sesión que se utilizará para cifrar toda la comunicación.

Aunque es posible utilizar el sistema usando un único cifrado correspondiente a la tarjeta, no resulta recomendable dado que la respuesta de la tarjeta podría ser suplantada fácilmente, hecho que debilitaría considerablemente la seguridad del sistema.

Resulta evidente para el experto en la materia que este procedimiento es susceptible de numerosas variaciones y modificaciones, y que los detalles mencionados pueden ser sustituidos por otros técnicamente equivalentes, sin por ello apartarse del ámbito de protección definido por las reivindicaciones adjuntas.

código de autenticidad del mismo, realizándose unas terceras operaciones criptográficas adecuadas para la verificación de las utilizadas en la generación del documento, siendo imprescindible la participación activa del dispositivo verificador portátil asociado para la validación del documento y almacenando el verificador portátil una lista de los documentos que ha verificado de manera que es posible saber, al menos, si se trata de la primera validación.

3ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la citada etapa de individualización de los dispositivos verificadores portátiles se realiza almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las de un algoritmo de cifrado simétrico o de clave secreta;
- dicha primera y segunda operación criptográfica comprenden dos cifrados mediante un algoritmo criptográfico simétrico con la clave del grupo de lectores/verificadores/grabadores que participan en la validación del documento y otro algoritmo criptográfico simétrico con la clave correspondiente del dispositivo verificador portátil asociado al documento; y en que
- dichas terceras operaciones criptográficas comprenden el descifrado, por parte del dispositivo verificador portátil con su clave correspondiente, del código de autenticidad del documento y el descifrado subsiguiente, por parte del citado lector/verificador/grabador con su clave correspondiente, realizándose ambos descifrados mediante algoritmos criptográficos simétricos.

4ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores

portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende una firma digital con una clave secreta, de la cual los citados lectores/verificadores/grabadores que participan en la validación del documento conocen su correspondiente pública, y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y en que

- las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una comprobación de firma, con la clave pública correspondiente almacenada en los lectores/verificadores/grabadores.

5ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende un cifrado con la clave pública de los lectores/verificadores/grabadores que participan en la validación del documento y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y

-las citadas terceras operaciones criptográficas se basan

en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una descifrado con la clave secreta de dichos lectores/verificadores/grabadores.

6ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública;

- dicha primera y segunda operación criptográfica se basan en criptografía de clave pública que comprende una firma digital con la clave secreta correspondiente a la clave pública almacenada en los citados lectores/verificadores/grabadores que participan en la validación del documento y otra firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y en que

- las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende la comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y otra comprobación de firma con la clave pública correspondiente de los lectores/verificadores/grabadores.

7ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves

las públicas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basan en criptografía de clave pública que comprende un cifrado con la clave pública correspondiente a la clave secreta almacenada en dichos lectores/verificadores/grabadores que participan en la validación del documento y una firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y en que

- dichas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende una comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y un descifrado con la clave secreta correspondiente de los citados lectores/verificadores/grabadores.

8ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que comprende la comprobación, antes de validar el documento, de que éste no se encuentra en la lista de documentos validados.

9ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 8ª, caracterizado en que comprende la indicación al lector/grabador/verificador de que el documento a validar se encuentra en la lista de documentos validados para que éste tome las medidas oportunas.

10ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 8ª, caracterizado en que comprende la inclusión del documento en la lista de documentos validados en el caso de que el documento a validar no se encuentre en la misma, realizándose la operación criptográfica correspondiente a invertir y/o

comprobar la operación criptográfica correspondiente al dispositivo verificador portátil, enviando el resultado al lector/grabador/verificador para que tome las medidas oportunas.

11ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en la autentificación criptográfica establecida entre el citado dispositivo verificador portátil y el lector/grabador/verificador es una autentificación criptográfica mutua fuerte.

12ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 11ª, caracterizado en que entre el dispositivo verificador portátil y el lector/grabador/verificador se establece una clave de sesión cooperativa y aleatoria utilizada para cifrar los mensajes pertinentes entre ambos.

13ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado en que la etapa de individualización de los dispositivos verificadores portátiles por parte de sus emisores se realiza mediante una o varias claves que se obtienen a partir del cifrado del número de serie con una o varias claves maestras elegidas por los operadores de dispositivos verificadores portátiles, de manera que la clave maestra de cada operador y el dispositivo verificador portátil corresponde con su identificador, apareciendo dicho identificador de una manera legible para el usuario.

14ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado en que el citado lector/verificador/grabador está adaptado para emitir una información admitiendo o rechazando el documento e informando de la causa.

15ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado

en que las claves del lector/verificador/grabador son comunes a un conjunto de lectores.

16ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que las claves almacenadas en los lectores/verificadorer/grabadores se obtienen cifrando sus identificadores o parte de ellos con unas claves maestras elegidas por sus operadores.

17ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 1ª reivindicación, caracterizado en que en los documentos que presentan fecha de caducidad, ésta se incorpora en el código de autenticidad, de manera que pueden ser eliminados de la lista de documentos validados almacenada en dicho verificador portátil una vez que éstos han caducado.

18ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 17ª, caracterizado en que los citados dispositivos verificadores portátiles adquieren la fecha para borrar los documentos caducados de la lista de documentos validados por medio de un certificado digital emitido por una entidad competente.

19ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que la selección y obtención del documento y/o su código de autenticidad se realiza a través de Internet.

20ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad del documento se envía al teléfono móvil del usuario.

21ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad del documento se envía a una agenda electrónica o similar del usuario.

22ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código de barras.

23ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante varios código de barras.

24ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código alfanumérico.

25ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código de puntos.

26ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualesquiera de las reivindicaciones 22ª a 25ª, caracterizado en que el código de autenticidad se imprime también en modo alfanumérico para poder realizar una entrada manual del mismo en caso de deterioro del código de lectura automática.

27ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 23ª caracterizado en que en los códigos de barras incluyen el orden correcto de lectura.